Burp Scanner Report

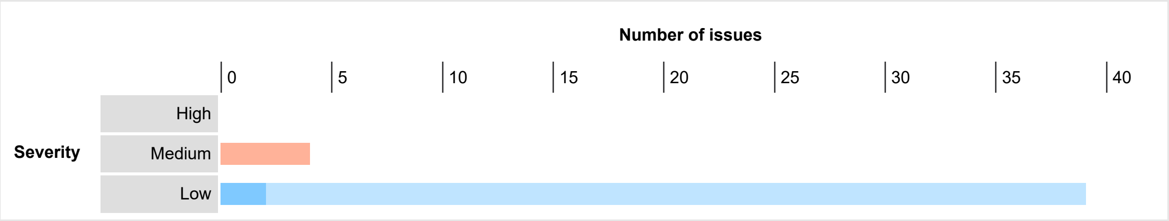
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	4	0	4
	Low	0	2	37	39
	Information	3	2	0	5

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. Session token in URL

There are 4 instances of this issue:

- /signalr/connect
- /signalr/connect
- /signalr/poll
- /signalr/start

Issue background

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request

1.1. https://portal.simetric.com/signalr/connect

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://portal.simetric.com**
Path:	**/signalr/connect**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://portal.simetric.com/signalr/connect?transport=longPolling&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOpdqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D

Request

```
POST /signalr/connect?
transport=longPolling&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOp
dqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgl_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Content-Length: 0
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://portal.simetric.com
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/DataManagement/AsyncRequests
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=UTF-8
Expires: -1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:33:25 GMT

{"C":"d-B6A9B51C-B,0|G,0|H,2","S":1,"M":[]}
```

1.2. https://portal.simetric.com/signalr/connect

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://portal.simetric.com**
Path:	**/signalr/connect**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://portal.simetric.com/signalr/connect?transport=serverSentEvents&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOpdqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D&tid=9

Request

```
GET /signalr/connect?
transport=serverSentEvents&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1G
hXvOpdqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D&tid=9 HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: text/event-stream
Cache-Control: no-cache
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/DataManagement/AsyncRequests
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/event-stream
Expires: -1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
```

```
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:33:18 GMT

data: initialized

data: {"C":"d-B6A9B51C-B,0|G,0|H,1","S":1,"M":[]}

data: {}
```

1.3. https://portal.simetric.com/signalr/poll

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://portal.simetric.com**
Path:	**/signalr/poll**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://portal.simetric.com/signalr/poll?transport=longPolling&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOpdqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D

Request

```
POST /signalr/poll?
transport=longPolling&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOp
dqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Content-Length: 42
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://portal.simetric.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/DataManagement/AsyncRequests
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

messageId=d-B6A9B51C-B%2C0%7CG%2C0%7CH%2C2
```

Response

```
HTTP/2 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=UTF-8
Expires: -1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:33:26 GMT

{"C":"d-B6A9B51C-B,0|G,1|H,2","M":[{"H":"SignalRNotificationHub","M":"onConnected","A":[]}]}
```

1.4. https://portal.simetric.com/signalr/start

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://portal.simetric.com**
Path:	**/signalr/start**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://portal.simetric.com/signalr/start?transport=longPolling&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOpdqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D&_=1625470382278

Request

```
GET /signalr/start?
transport=longPolling&clientProtocol=2.1&connectionToken=gKaW6IHjFRHCCwLDlvA5Om8KvDoG%2FiGvayBh2JC4bOCAZlgAP7%2BMjE9LYGGBzv3xrXXDmhItB0JFw6HXW1GhXvOp
dqUPHI0z2cdAKV2eTNVshbvj3nMsjbRoU0Sohdvq&connectionData=%5B%7B%22name%22%3A%22signalrnotificationhub%22%7D%5D&_=1625470382278 HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type: application/json; charset=UTF-8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/DataManagement/AsyncRequests
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=UTF-8
Expires: -1
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:33:26 GMT

{ "Response": "started" }
```

2. Open redirection (DOM-based)

There are 37 instances of this issue:

- /simetric/Account
- /simetric/Account
- /simetric/Actions/SimManagement
- /simetric/AdHocReport
- /simetric/AdHocReport
- /simetric/Administration/JobConsole
- /simetric/Administration/JobConsole
- /simetric/Analytics/Dashboard
- /simetric/Customers
- /simetric/Customers

- /simetric/DataManagement/AsyncRequests
- /simetric/DataManagement/AsyncRequests
- /simetric/DataManagement/DataSource
- /simetric/DataManagement/manualupload
- /simetric/DataManagement/manualupload
- /simetric/DataManagement/manualupload
- /simetric/InvoiceDetails/Index
- /simetric/InvoiceDetails/Index
- /simetric/Notification/CustomRules
- /simetric/Notification/CustomRules
- /simetric/Notification/NotificationSetup
- /simetric/Notification/ScheduledReport
- /simetric/Notification/WatchLists
- /simetric/Notification/WatchLists
- /simetric/Optimization/History
- /simetric/Optimization/History
- /simetric/Optimization/Preview
- /simetric/Optimization/Preview
- /simetric/Research/ChangeHistory
- /simetric/Research/SMSHistory
- /simetric/SIMs/Exceptions
- /simetric/SIMs/Exceptions
- /simetric/SIMs/Exceptions
- /simetric/Sims/Assignment
- /simetric/Sims/Segmentation
- /simetric/Sims/Segmentation
- /simetric/Sims/Segmentation

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Note: If an attacker is able to control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Vulnerability classifications

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

2.1. https://portal.simetric.com/simetric/Account

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Account**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Account HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/InvoiceDetails/Index
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 82347
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:29 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Account//w3dg1a5rgi%27%22%60'%22/w3dg1a5rgi/%3E%3Cw3dg1a5rgi//%3Eq2n2zd6k0k&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Eq2n2zd6k0k&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Account:1746:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Account:1746:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.2. https://portal.simetric.com/simetric/Account

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Account**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/Account HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
```

```
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/InvoiceDetails/Index
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 82347
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:29 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.3. https://portal.simetric.com/simetric/Actions/SimManagement

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Actions/SimManagement**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Actions/SimManagement HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Notification/ScheduledReport
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 82311
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:28:57 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Actions/SimManagement//w2cviaudx3%27%22%60'%22/w2cviaudx3/%3E%3Cw2cviaudx3//%3Ecfwt901126&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ecfwt901126&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Actions/SimManagement:1523:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Actions/SimManagement:1523:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.4. https://portal.simetric.com/simetric/AdHocReport

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/AdHocReport**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/AdHocReport HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgl_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Notification/CustomRules
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 94964
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:27:06 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/AdHocReport//p8oz36ejlh%27%22%60'%22/p8oz36ejlh/%3E%3Cp8oz36ejlh//%3Eybj6d0vyel&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Eybj6d0vyel&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/AdHocReport:1573:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/AdHocReport:1573:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.5. https://portal.simetric.com/simetric/AdHocReport

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/AdHocReport**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.open**.

Request

```
GET /simetric/AdHocReport HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Notification/CustomRules
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 94964
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:27:06 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.open**.

The source element has id **CompanyId** and name **Company.CompanyId**.

The following value was injected into the source:

```
97
```

The previous value reached the sink as:

```
/Notification/DetectNotificationChange?companyId=gyhenx4lvp%2527%2522`'"/gyhenx4lvp/><gyhenx4lvp/\>azd7gfj971&&currentCount=undefined&currentTimeStamp=unde
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:67:41)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:70:11)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.6. https://portal.simetric.com/simetric/Administration/JobConsole

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Administration/JobConsole**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Administration/JobConsole HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/DataManagement/DataSource
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 51325
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
```

```
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:01 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Administration/JobConsole//toijc1cemm%27%22%60'%22/toijc1cemm/%3E%3Ctoijc1cemm//%3Ezdgtqjiwkg&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ezdgtqjiwkg&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Administration/JobConsole:1092:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Administration/JobConsole:1092:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.7. https://portal.simetric.com/simetric/Administration/JobConsole

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Administration/JobConsole**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/Administration/JobConsole HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0elhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYl93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/DataManagement/DataSource
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 51325
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:01 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.8. https://portal.simetric.com/simetric/Analytics/Dashboard

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Analytics/Dashboard**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Analytics/Dashboard HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Referer: https://portal.simetric.com/?state=197a74e9-30eb-4f39-a90f-
08cf977cbd3f&code=eyJraWQiOiJjcGltY29yZV8wOTI1MjAxNSIsInZlciI6IjEuMCIsInppcCI6IkRlZmxhdGUiLCJzZXIiOiIxLjAifQ..yOFYwap66MoQQ2Tb.PSney3iGIy0G4Obm79liHpyBKVID2Y
rm1WdqtjogvS_d5JS77drBM8SG8pDc7x-Pje_iepaEDLbKLPLaye5pju67GqKP99djB7X-mOE_5ZG748FpHcdnCu-
1izOtwxUeB37x3zy1ous0FHJAL7cLrsmQlB8XLiucLfOto4hHZugJBgDZzu5z-xDjeDtGefK9YojeMJykiRT3molTobiazlsy_IFNTvDvjxJlOImoba3zJ8nenANtslf5EV7AO1oZIhQjHK-
rW_vL8ADSD-
hhIXMTv15_DgvwMsumDx9kGCXjdThlV19h2k7KOBJMKvd0qgotziCo906L23yPklWxrljL2aZ76yZGcAykgNrIworUUVCorE2Mx2QgxoOkfjxNlUmQ2dnL7pBWsmNambbiaY5h72webjmxBP6y
-q7D77XBxTpQ_ESRlpeyvDLF9DM_h2LNafDcYxkSxpWD1DPQ_u217GC7vMaT5UkNi1Ca07YcKxOpveNh_IYoQieW1DKB-H_gGMiUr14qNj-
Dm8hMc8rgNVXGzYYAguuBMjeGiLfz8hKDgzF8Hksf9ZxOb7CUE38JFSuXtxrjy12id7lkBDK68T2jem6qVesxECtBWW_CegEJ-KOofgbaHlI98XSSq0I2Tq29Bx6mRTsl4-
BpG3jSaVYWbQhd2-3EPlsrsRvUMuneeZg-ulUd_MZBurcGb8mBoxu60X8PRAbM96HEOfMH8JxF48E-v85eoXIEP73CqoukaN2-S8eoPOwG._kXmk8hr0_pD5OmLyhdx4g
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 50440
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:24:20 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Analytics/Dashboard//w4i1brwz9n%27%22%60'%22/w4i1brwz9n/%3E%3Cw4i1brwz9n//%3Es7kbwm8i7q&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Es7kbwm8i7q&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Analytics/Dashboard:852:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Analytics/Dashboard:852:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.9. https://portal.simetric.com/simetric/Customers

Summary

Severity:	**Low**
Confidence:	**Tentative**

Host:	**https://portal.simetric.com**
Path:	**/simetric/Customers**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Customers HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXIeINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 52836
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:34 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Customers//mumaej08r5%27%22%60'%22/mumaej08r5/%3E%3Cmumaej08r5//%3Etkiz8rrx9r&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Etkiz8rrx9r&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Customers:1133:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Customers:1133:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.10. https://portal.simetric.com/simetric/Customers

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Customers**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/Customers HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 52836
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:34 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.11. https://portal.simetric.com/simetric/DataManagement/AsyncRequests

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/DataManagement/AsyncRequests**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/DataManagement/AsyncRequests HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Sims/Assignment
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 101600
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:58 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/DataManagement/AsyncRequests//d8m86kkzq1%27%22%60'%22/d8m86kkzq1/%3E%3Cd8m86kkzq1//%3Ezc006uc84v&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ezc006uc84v&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/DataManagement/AsyncRequests:1928:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/DataManagement/AsyncRequests:1928:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.12. https://portal.simetric.com/simetric/DataManagement/AsyncRequests

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/DataManagement/AsyncRequests**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/DataManagement/AsyncRequests HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Sims/Assignment
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 101600
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:58 GMT

<!DOCTYPE html>
<html>
```

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.13. https://portal.simetric.com/simetric/DataManagement/DataSource

Summary

?	Severity:	**Low**
	Confidence:	**Tentative**
	Host:	**https://portal.simetric.com**
	Path:	**/simetric/DataManagement/DataSource**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/DataManagement/DataSource HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/DataManagement/AsyncRequests
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 52740
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:40:34 GMT
```

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/DataManagement/DataSource//l7e3x6x8uw%27%22%60'%22/l7e3x6x8uw/%3E%3Cl7e3x6x8uw//%3Ejokipy2fm4&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ejokipy2fm4&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/DataManagement/DataSource:1070:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/DataManagement/DataSource:1070:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.14. https://portal.simetric.com/simetric/DataManagement/manualupload

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/DataManagement/manualupload**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/DataManagement/manualupload HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Administration/JobConsole
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 59795
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:12 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/DataManagement/manualupload//y888vwph4f%27%22%60'%22/y888vwph4f/%3E%3Cy888vwph4f//%3Edo0gge19mg&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Edo0gge19mg&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/DataManagement/manualupload:1120:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/DataManagement/manualupload:1120:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.15. https://portal.simetric.com/simetric/DataManagement/manualupload

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/DataManagement/manualupload**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.open**.

Request

```
GET /simetric/DataManagement/manualupload HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
```

```
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Administration/JobConsole
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 59795
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:12 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.open**.

The source element has id **CompanyId** and name **Company.CompanyId**.

The following value was injected into the source:

```
97
```

The previous value reached the sink as:

```
/Notification/DetectNotificationChange?companyId=l47hm38y8o%2527%2522`'"/l47hm38y8o/><l47hm38y8o/\>iphb5y2w1h&&currentCount=undefined&currentTimeStamp=unde
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:67:41)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:70:11)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.16. https://portal.simetric.com/simetric/DataManagement/manualupload

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/DataManagement/manualupload**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/DataManagement/manualupload HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Administration/JobConsole
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 59795
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:12 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`

- `location.href = url;`

2.17. https://portal.simetric.com/simetric/InvoiceDetails/Index

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/InvoiceDetails/Index**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/InvoiceDetails/Index HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/SIMs/Exceptions
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 182603
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:05 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/InvoiceDetails/Index//g8p6vxehh5%27%22%60'%22/g8p6vxehh5/%3E%3Cg8p6vxehh5//%3Ec3evgis1jx&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ec3evgis1jx&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/InvoiceDetails/Index:4026:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/InvoiceDetails/Index:4026:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.18. https://portal.simetric.com/simetric/InvoiceDetails/Index

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/InvoiceDetails/Index**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/InvoiceDetails/Index HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/SIMs/Exceptions
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 182603
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:05 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

```
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.19. https://portal.simetric.com/simetric/Notification/CustomRules

Summary

?	Severity:	**Low**
	Confidence:	**Tentative**
	Host:	**https://portal.simetric.com**
	Path:	**/simetric/Notification/CustomRules**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Notification/CustomRules HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Notification/NotificationSetup
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 98912
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:26:24 GMT

<!DOCTYPE html>
<html>
```

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
```
...[SNIP]...

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Notification/CustomRules//r2lmmpbpok%27%22%60'%22/r2lmmpbpok/%3E%3Cr2lmmpbpok//%3Enki2cce2wx&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Enki2cce2wx&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/CustomRules:1581:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/CustomRules:1581:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.20. https://portal.simetric.com/simetric/Notification/CustomRules

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Notification/CustomRules**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.open**.

Request

```
GET /simetric/Notification/CustomRules HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgl_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Notification/NotificationSetup
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 98912
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:26:24 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.open**.

The source element has id **CompanyId** and name **Company.CompanyId**.

The following value was injected into the source:

```
97
```

The previous value reached the sink as:

```
/Notification/DetectNotificationChange?companyId=u78jipqxlf%2527%2522`'"/u78jipqxlf/><u78jipqxlf/\>lglowcy13p&&currentCount=undefined&currentTimeStamp=unde
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:67:41)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:70:11)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.21. https://portal.simetric.com/simetric/Notification/NotificationSetup

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Notification/NotificationSetup**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Notification/NotificationSetup HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Analytics/Dashboard
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 268126
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:26:16 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Notification/NotificationSetup//hc536u3l5u%27%22%60'%22/hc536u3l5u/%3E%3Chc536u3l5u//%3Ej3hqs3b0p9&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ej3hqs3b0p9&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/NotificationSetup:1694:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/NotificationSetup:1694:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.22. https://portal.simetric.com/simetric/Notification/ScheduledReport

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Notification/ScheduledReport**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Notification/ScheduledReport HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgl_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Research/SMSHistory
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 47689
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:27:48 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Notification/ScheduledReport//pwagoygjad%27%22%60'%22/pwagoygjad/%3E%3Cpwagoygjad//%3Ezojfigizeq&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ezojfigizeq&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/ScheduledReport:963:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/ScheduledReport:963:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.23. https://portal.simetric.com/simetric/Notification/WatchLists

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Notification/WatchLists**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Notification/WatchLists HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Sims/Segmentation
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 75245
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:48 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Notification/WatchLists//tgj0ta182a%27%22%60'%22/tgj0ta182a/%3E%3Ctgj0ta182a//%3Evxqfb1y9am&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Evxqfb1y9am&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/WatchLists:1418:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Notification/WatchLists:1418:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.24. https://portal.simetric.com/simetric/Notification/WatchLists

Summary

?	Severity:	**Low**
	Confidence:	**Tentative**
	Host:	**https://portal.simetric.com**
	Path:	**/simetric/Notification/WatchLists**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.open**.

Request

```
GET /simetric/Notification/WatchLists HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Sims/Segmentation
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 75245
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:48 GMT
```

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
```
...[SNIP]...

Dynamic analysis

Data is read from **input.value** and passed to **xhr.open**.

The source element has id **CompanyId** and name **Company.CompanyId**.

The following value was injected into the source:

```
97
```

The previous value reached the sink as:

```
/Notification/DetectNotificationChange?companyId=nfel0xtp3y%2527%2522`'"/nfel0xtp3y/><nfel0xtp3y/\>q5wm3scvsa&&currentCount=undefined&currentTimeStamp=unde
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:67:41)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:70:11)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.25. https://portal.simetric.com/simetric/Optimization/History

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Optimization/History**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Optimization/History HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Optimization/Preview
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 46632
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:57 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Optimization/History//h21s3uae9n%27%22%60'%22/h21s3uae9n/%3E%3Ch21s3uae9n//%3Eaiziip0nuf&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Eaiziip0nuf&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Optimization/History:931:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Optimization/History:931:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.26. https://portal.simetric.com/simetric/Optimization/History

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Optimization/History**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/Optimization/History HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Optimization/Preview
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 46632
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:57 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.27. https://portal.simetric.com/simetric/Optimization/Preview

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Optimization/Preview**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Optimization/Preview HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/DataManagement/manualupload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 93686
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:43 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Optimization/Preview//ppyvkptva4%27%22%60'%22/ppyvkptva4/%3E%3Cppyvkptva4//%3Ed1h371avwg&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ed1h371avwg&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Optimization/Preview:1849:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Optimization/Preview:1849:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.28. https://portal.simetric.com/simetric/Optimization/Preview

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Optimization/Preview**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/Optimization/Preview HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/DataManagement/manualupload
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 93686
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:44:43 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`

- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.29. https://portal.simetric.com/simetric/Research/ChangeHistory

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Research/ChangeHistory**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Research/ChangeHistory HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/AdHocReport
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 41698
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:27:36 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

`///simetric/Research/ChangeHistory//x7b41heucf%27%22%60'%22/x7b41heucf/%3E%3Cx7b41heucf//%3Epvqxrbbcv3&`

The previous value reached the sink as:

`/Landing/LoadHelp?page=%3Epvqxrbbcv3&`

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Research/ChangeHistory:809:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Research/ChangeHistory:809:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.30. https://portal.simetric.com/simetric/Research/SMSHistory

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Research/SMSHistory**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Research/SMSHistory HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XICJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Research/ChangeHistory
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 42202
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:27:46 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
```

```
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Research/SMSHistory//eluf4x0e5a%27%22%60'%22/eluf4x0e5a/%3E%3Celuf4x0e5a//%3Esb8xv5hg6a&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Esb8xv5hg6a&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Research/SMSHistory:809:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Research/SMSHistory:809:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.31. https://portal.simetric.com/simetric/SIMs/Exceptions

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/SIMs/Exceptions**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.send**.

Request

```
GET /simetric/SIMs/Exceptions HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Optimization/History
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 65477
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:45:37 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.send**.

The source element has id **CompanyNumber** and name **Company.CompanyNumber**.

The following value was injected into the source:

```
simetric
```

The previous value reached the sink as:

```
{"typeId":"116","companyNumber":"uubf6eypli%2527%2522`'\"/uubf6eypli/><uubf6eypli/\\>hwxbnkxi7f&","connectionId":"3"}
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at PreviewRestrictedDevices (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:243:44)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:21:9)
at HTMLDocument.dispatch (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:48638)
at HTMLDocument.a.handle (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:46737)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:70565)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71118)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71094)
at Object.i.fn.<computed> [as click] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71530)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/SIMs/Exceptions:1232:39)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at Object.IQlSq (<anonymous>:1:833965)
at XMLHttpRequest._0x38c034.XMLHttpRequest.<computed> [as send] (<anonymous>:1:835049)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79962)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at PreviewRestrictedDevices (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:247:7)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:21:9)
at HTMLDocument.dispatch (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:48638)
at HTMLDocument.a.handle (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:46737)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:70565)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71118)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71094)
at Object.i.fn.<computed> [as click] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71530)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/SIMs/Exceptions:1232:39)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.32. https://portal.simetric.com/simetric/SIMs/Exceptions

Summary

Severity:	**Low**
Confidence:	**Tentative**

Host:	**https://portal.simetric.com**
Path:	**/simetric/SIMs/Exceptions**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/SIMs/Exceptions HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgl_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Optimization/History
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 65477
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:45:37 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/SIMs/Exceptions//ecaxcfclx2%27%22%60'%22/ecaxcfclx2/%3E%3Cecaxcfclx2//%3Ea84qeym2gs&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ea84qeym2gs&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/SIMs/Exceptions:1188:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/SIMs/Exceptions:1188:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.33. https://portal.simetric.com/simetric/SIMs/Exceptions

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/SIMs/Exceptions**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/SIMs/Exceptions HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Optimization/History
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 65477
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:45:37 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

2.34. https://portal.simetric.com/simetric/Sims/Assignment

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Sims/Assignment**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Sims/Assignment HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Notification/WatchLists
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 48670
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:54 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

`///simetric/Sims/Assignment//fchm1yll1q%27%22%60'%22/fchm1yll1q/%3E%3Cfchm1yll1q//%3Ek1s5imuzfg&`

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ek1s5imuzfg&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Sims/Assignment:824:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Sims/Assignment:824:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.35. https://portal.simetric.com/simetric/Sims/Segmentation

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Sims/Segmentation**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **xhr.open**.

Request

```
GET /simetric/Sims/Segmentation HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Actions/SimManagement
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 108357
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:20 GMT

<!DOCTYPE html>
<html>
```

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **xhr.open**.

The following value was injected into the source:

```
///simetric/Sims/Segmentation//k7tjgocvl1%27%22%60'%22/k7tjgocvl1/%3E%3Ck7tjgocvl1//%3Ekqpbwcbzv6&
```

The previous value reached the sink as:

```
/Landing/LoadHelp?page=%3Ekqpbwcbzv6&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Sims/Segmentation:1728:38)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at loadHelpContent (https://portal.simetric.com/Scripts/common.js?v=1.0.7856.21182:226:7)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Sims/Segmentation:1728:13)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.36. https://portal.simetric.com/simetric/Sims/Segmentation

Summary

?	Severity:	**Low**
	Confidence:	**Tentative**
	Host:	**https://portal.simetric.com**
	Path:	**/simetric/Sims/Segmentation**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **input.value** and passed to **xhr.open**.

Request

```
GET /simetric/Sims/Segmentation HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Actions/SimManagement
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 108357
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:20 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **xhr.open**.

The source element has id **CompanyId** and name **Company.CompanyId**.

The following value was injected into the source:

```
97
```

The previous value reached the sink as:

```
/Notification/DetectNotificationChange?companyId=und97uvku7%2527%2522`'"/und97uvku7/><und97uvku7/\>rocku001sj&&currentCount=undefined&currentTimeStamp=unde
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:67:41)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.efGJl (<anonymous>:1:811973)
at XMLHttpRequest._0x38c034.<computed>.<computed>.<computed> [as open] (<anonymous>:1:833024)
at Object.send (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:79140)
at Function.ajax (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:76424)
at Arguments.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:70:11)
at <anonymous>:1:866060
at DetectNotificationChange (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:66:5)
at HTMLDocument.<anonymous> (https://portal.simetric.com/Scripts/newnotificationheader.js?v=1.0.7856.21182:3:5)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

2.37. https://portal.simetric.com/simetric/Sims/Segmentation

Summary

?	Severity:	**Low**
	Confidence:	**Tentative**
	Host:	**https://portal.simetric.com**
	Path:	**/simetric/Sims/Segmentation**

Issue detail

The application may be vulnerable to DOM-based open redirection. Data is read from **location.pathname** and passed to **location.href**.

Request

```
GET /simetric/Sims/Segmentation HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Actions/SimManagement
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 108357
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:20 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
).val("Imei");
break;
}
// $('#iccidSearchSubmit').trigger('click');
}
});
function changeCompany(companyNumber) {
var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);
url = location.protocol + "//" + location.host + url;
location.href = url;
}
</script>
...[SNIP]...
```

Static analysis

Data is read from **location.pathname** and passed to **location.href** via the following statements:

- `var url = location.pathname.replace(location.pathname.split("/")[1], companyNumber);`
- `url = location.protocol + "//" + location.host + url;`
- `location.href = url;`

3. Client-side HTTP parameter pollution (reflected)

There are 2 instances of this issue:

- /Landingpage/Initiate/aee899f1-c16b-43a8-9d47-e81ebb7b2f0d [URL path folder 2]
- /simetric/Analytics/Dashboard [URL path folder 2]

Issue background

Client-side HTTP parameter pollution (HPP) vulnerabilities arise when an application embeds user input in URLs in an unsafe manner. An attacker can use this vulnerability to construct a URL that, if visited by another application user, will modify URLs within the response by inserting additional query string parameters and sometimes overriding existing ones. This may result in links and forms having unexpected side effects. For example, it may be possible to modify an invitation form using HPP so that the invitation is delivered to an unexpected recipient.

The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

References

- HTTP Parameter Pollution

Vulnerability classifications

- CWE-233: Improper Handling of Parameters
- CWE-20: Improper Input Validation

3.1. https://portal.simetric.com/Landingpage/Initiate/aee899f1-c16b-43a8-9d47-e81ebb7b2f0d [URL path folder 2]

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://portal.simetric.com**
Path:	**/Landingpage/Initiate/aee899f1-c16b-43a8-9d47-e81ebb7b2f0d**

Issue detail

The value of the URL path folder 2 is copied into the response within the query string of a URL.

The payload **zeq&rzt=1** was submitted in the URL path folder 2. This input was echoed unmodified within the response header **Location**.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary query string parameters into URLs in the application's response.

Request

```
GET /Landingpage/zeq%26rzt%3d1/aee899f1-c16b-43a8-9d47-e81ebb7b2f0d HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/?state=197a74e9-30eb-4f39-a90f-
08cf977cbd3f&code=eyJraWQiOiJjcGltY29yZV8wOTI1MjAxNSIsInZlciI6IjEuMCIsInppcCI6IkRlZmxhdGUiLCJzZXIiOiIxLjAifQ..yOFYwap66MoQQ2Tb.PSney3iGIy0G4Obm79liHpyBKVID2Y
rm1WdqtjogvS_d5JS77drBM8SG8pDc7x-Pje_iepaEDLbKLPLaye5pju67GqKP99djB7X-mOE_5ZG748FpHcdnCu-
1izOtwxUeB37x3zy1ous0FHJAL7cLrsmQlB8XLiucLfOto4hHZugJBgDZzu5z-xDjeDtGefK9YojeMJykiRT3molTobiazlsy_IFNTvDvjxJlOImoba3zJ8nenANtslf5EV7AO1oZIhQjHK-
rW_vL8ADSD-
hhIXMTv15_DgvwMsumDx9kGCXjdThlV19h2k7KOBJMKvd0qgotziCo906L23yPklWxrljL2aZ76yZGcAykgNrIworUUVCorE2Mx2QgxoOkfjxNlUmQ2dnL7pBWsmNambbiaY5h72webjmxBP6y
-q7D77XBxTpQ_ESRlpeyvDLF9DM_h2LNafDcYxkSxpWD1DPQ_u217GC7vMaT5UkNi1Ca07YcKxOpveNh_IYoQieW1DKB-H_gGMiUr14qNj-
Dm8hMc8rgNVXGzYYAguuBMjeGiLfz8hKDgzF8Hksf9ZxOb7CUE38JFSuXtxrjy12id7lkBDK68T2jem6qVesxECtBWW_CegEJ-KOofgbaHlI98XSSq0I2Tq29Bx6mRTsl4-
BpG3jSaVYWbQhd2-3EPlsrsRvUMuneeZg-ulUd_MZBurcGb8mBoxu60X8PRAbM96HEOfMH8JxF48E-v85eoXIEP73CqoukaN2-S8eoPOwG._kXmk8hr0_pD5OmLyhdx4g
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 302 Found
Cache-Control: private
Content-Length: 210
Content-Type: text/html; charset=utf-8
Location: /Error/NotFound?aspxerrorpath=/Landingpage/zeq&rzt=1/aee899f1-c16b-43a8-9d47-e81ebb7b2f0d
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:54:04 GMT

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error/NotFound?aspxerrorpath=/Landingpage/zeq&amp;rzt=1/aee899f1-c16b-43a8-9d47-e81ebb7b2f0d">here</a>.</h2>
</body
...[SNIP]...
```

3.2. https://portal.simetric.com/simetric/Analytics/Dashboard [URL path folder 2]

Summary

Severity:	**Low**
Confidence:	**Firm**
Host:	**https://portal.simetric.com**
Path:	**/simetric/Analytics/Dashboard**

Issue detail

The value of the URL path folder 2 is copied into the response within the query string of a URL.

The payload **tox&jib=1** was submitted in the URL path folder 2. This input was echoed unmodified within the response header **Location**.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary query string parameters into URLs in the application's response.

Request

```
GET /simetric/tox%26jib%3d1/Dashboard HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Referer: https://portal.simetric.com/?state=197a74e9-30eb-4f39-a90f-
08cf977cbd3f&code=eyJraWQiOiJjcGltY29yZV8wOTI1MjAxNSIsInZlciI6IjEuMCIsInppcCI6IkRlZmxhdGUiLCJzZXIiOiIxLjAifQ..yOFYwap66MoQQ2Tb.PSney3iGIy0G4Obm79liHpyBKVID2Y
rm1WdqtjogvS_d5JS77drBM8SG8pDc7x-Pje_iepaEDLbKLPLaye5pju67GqKP99djB7X-mOE_5ZG748FpHcdnCu-
1izOtwxUeB37x3zy1ous0FHJAL7cLrsmQlB8XLiucLfOto4hHZugJBgDZzu5z-xDjeDtGefK9YojeMJykiRT3molTobiazlsy_IFNTvDvjxJlOImoba3zJ8nenANtslf5EV7AO1oZIhQjHK-
rW_vL8ADSD-
hhIXMTv15_DgvwMsumDx9kGCXjdThlV19h2k7KOBJMKvd0qgotziCo906L23yPklWxrljL2aZ76yZGcAykgNrIworUUVCorE2Mx2QgxoOkfjxNlUmQ2dnL7pBWsmNambbiaY5h72webjmxBP6y
-q7D77XBxTpQ_ESRlpeyvDLF9DM_h2LNafDcYxkSxpWD1DPQ_u217GC7vMaT5UkNi1Ca07YcKxOpveNh_IYoQieW1DKB-H_gGMiUr14qNj-
Dm8hMc8rgNVXGzYYAguuBMjeGiLfz8hKDgzF8Hksf9ZxOb7CUE38JFSuXtxrjy12id7lkBDK68T2jem6qVesxECtBWW_CegEJ-KOofgbaHlI98XSSq0I2Tq29Bx6mRTsl4-
BpG3jSaVYWbQhd2-3EPlsrsRvUMuneeZg-ulUd_MZBurcGb8mBoxu60X8PRAbM96HEOfMH8JxF48E-v85eoXIEP73CqoukaN2-S8eoPOwG._kXmk8hr0_pD5OmLyhdx4g
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 302 Found
Content-Length: 180
Content-Type: text/html; charset=utf-8
Location: /Error/NotFound?aspxerrorpath=/simetric/tox&jib=1/Dashboard
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:54:03 GMT

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error/NotFound?aspxerrorpath=/simetric/tox&amp;jib=1/Dashboard">here</a>.</h2>
</body></html>
```

4. HTML5 storage manipulation (DOM-based)

Summary

Severity:	**Information**
Confidence:	**Firm**

Host:	**https://portal.simetric.com**
Path:	**/simetric/Account**

Issue detail

The application may be vulnerable to DOM-based HTML5 storage manipulation. Data is read from **location.pathname** and passed to **localStorage.setItem.name**.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

HTML5 storage manipulation arises when a script stores controllable data in the HTML5 storage of the web browser (either localStorage or sessionStorage). An attacker may be able to use this behavior to construct a URL that, if visited by another application user, will cause the user's browser to store attacker-controllable data.

This behavior does not in itself constitute a security vulnerability. However, if the application later reads the data back from storage and processes it in an unsafe way, then an attacker may be able to leverage the storage mechanism to deliver other DOM-based attacks, such as cross-site scripting and JavaScript injection.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Vulnerability classifications

- CWE-20: Improper Input Validation

Request

```
GET /simetric/Account HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/InvoiceDetails/Index
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 82347
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:29 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **location.pathname** and passed to **localStorage.setItem.name**.

The following value was injected into the source:

```
///simetric/Account//z0coss0xb3%27%22%60'%22/z0coss0xb3/%3E%3Cz0coss0xb3//%3Et3bq7t25ge&
```

The previous value reached the sink as:

```
DataTables_userList_///simetric/Account//z0coss0xb3%27%22%60'%22/z0coss0xb3/%3E%3Cz0coss0xb3//%3Et3bq7t25ge&
```

The stack trace at the source was:

```
at Object.RwPgE (<anonymous>:1:793178)
at Object.get pathname [as pathname] (<anonymous>:1:800428)
at Object.fnStateSaveCallback (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:69221)
at Object.bi (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:33850)
at https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:35786
at Proxy.map (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:15307)
at o (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:35735)
at ut (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:12915)
at ot (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:13160)
at ni (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:22065)
at HTMLTableElement.<anonymous> (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:46056)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.u [as dataTable] (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:40821)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Account:1559:24)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.wfrkw (<anonymous>:1:343106)
at Object.zyiSW (<anonymous>:1:829234)
at Storage.setItem (<anonymous>:1:830278)
at Object.fnStateSaveCallback (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:69174)
at Object.bi (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:33850)
at https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:35786
at Proxy.map (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:15307)
at o (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:35735)
at ut (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:12915)
at ot (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:13160)
at ni (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:22065)
at HTMLTableElement.<anonymous> (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:46056)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.u [as dataTable] (https://portal.simetric.com/bundles/datatables/js?v=CD_L-iIICCrApk3gZ-R_sGiugujuxBbYrb3KXz1QUww1:1:40821)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/Account:1559:24)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

5. DOM data manipulation (DOM-based)

Summary

ⓘ	Severity:	**Information**
	Confidence:	**Firm**
	Host:	**https://portal.simetric.com**
	Path:	**/simetric/SIMs/Exceptions**

Issue detail

The application may be vulnerable to DOM-based DOM data manipulation. Data is read from **input.value** and passed to **element.textContent**.

Issue background

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM data manipulation arises when a script writes controllable data to a field within the DOM that is used within the visible UI or client-side application logic. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the appearance or behavior of the client-side UI. An attacker may be able to leverage this to perform virtual defacement of the application, or possibly to induce the user to perform unintended actions.

Burp Suite automatically identifies this issue using static code analysis, which may lead to false positives that are not actually exploitable. The relevant code and execution paths should be reviewed to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

Vulnerability classifications

- CWE-20: Improper Input Validation

Request

```
GET /simetric/SIMs/Exceptions HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhlfOGo5udxcVAuQ6W18VEpflG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgl_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
```

```
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portal.simetric.com/simetric/Optimization/History
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 65477
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:45:37 GMT

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-e
...[SNIP]...
```

Dynamic analysis

Data is read from **input.value** and passed to **element.textContent**.

The source element has id **desc_116** and name **desc_116**.

The following value was injected into the source:

```
Devices on this list are moved to the specified Rate Plan and then not allowed to move while optimizing.
```

The previous value reached the sink as:

```
sa5p5uod7c%2527%2522`'"/sa5p5uod7c/><sa5p5uod7c/\>bwc0a3paz3&
```

The stack trace at the source was:

```
at HTMLInputElement.get (<anonymous>:1:762287)
at HTMLInputElement.get [as value] (<anonymous>:1:878526)
at Object.val (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:68666)
at setSelectedSeg (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:38:50)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:19:9)
at HTMLDocument.dispatch (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:48638)
at HTMLDocument.a.handle (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:46737)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:70565)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71118)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71094)
at Object.i.fn.<computed> [as click] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71530)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/SIMs/Exceptions:1232:39)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

The stack trace at the sink was:

```
at Object.ncaRF (<anonymous>:1:901021)
at HTMLDivElement.set [as textContent] (<anonymous>:1:902417)
at HTMLDivElement.<anonymous> (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:53826)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.<anonymous> (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:53733)
at a (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41608)
at Object.text (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:53670)
at setSelectedSeg (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:38:19)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/Scripts/device_exceptionlist.js?v=1.0.7856.21182:19:9)
at HTMLDocument.dispatch (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:48638)
at HTMLDocument.a.handle (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:46737)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:70565)
at HTMLSpanElement.<anonymous> (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71118)
at Function.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:14708)
at Object.each (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:12772)
at Object.trigger (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71094)
at Object.i.fn.<computed> [as click] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:71530)
at HTMLDocument.<anonymous> (https://portal.simetric.com/simetric/SIMs/Exceptions:1232:39)
at c (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:38521)
at Object.fireWith [as resolveWith] (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:39283)
at Function.ready (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:41071)
at HTMLDocument.vt (https://portal.simetric.com/bundles/jquery/js?v=Dko0RH9uheov6kXUIevjjayG1arOKaRR7jBZQCuISOw1:1:941)
```

This was triggered by a **DOMContentLoaded** event.

6. Email addresses disclosed

There are 3 instances of this issue:

- /InvoiceDetails/GetDetail
- /Notification/AddEditCustomRulePredicates
- /Notification/GetCustomRulePredicate

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Vulnerability classifications

- CWE-200: Information Exposure

6.1. https://portal.simetric.com/InvoiceDetails/GetDetail

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://portal.simetric.com**
Path:	**/InvoiceDetails/GetDetail**

Issue detail

The following email address was disclosed in the response:

- asif@connectedanalytics.com

Request

```
GET /InvoiceDetails/GetDetail?selectedInvoiceKey=4583 HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zfIxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ;
__RequestVerificationToken=L6MpYamwXyTO1HcY2v7v_ugUnbelmkJt1ad3Cxeg8jdC3dWee8QXE74iSW2jxtgbJMXleINSxltvq6jAUjBn3PWGIxue1IphwkwPb8ZusWc1
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/InvoiceDetails/Index
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
```

```
Content-Length: 15606
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:46:13 GMT

<div style="margin-top: 20px;">
<form action="/InvoiceDetails/UpdateInvoice" class="form-horizontal" data-ajax="true" data-ajax-begin="onBeginUpdateInvoice" data-ajax-complete="onCompleteUpdateInvoic
...[SNIP]...
<input htmlAttributes="{ class = form-control }" id="ModifiedBy" name="ModifiedBy" type="hidden" value="asif@connectedanalytics.com" />
...[SNIP]...
```

6.2. https://portal.simetric.com/Notification/AddEditCustomRulePredicates

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://portal.simetric.com**
Path:	**/Notification/AddEditCustomRulePredicates**

Issue detail

The following email address was disclosed in the response:

- ganesh.jagdale@aszroh.com

Request

```
POST /Notification/AddEditCustomRulePredicates HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpfIG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Content-Length: 733
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Content-Type: application/json; charset=UTF-8
Origin: https://portal.simetric.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/AdHocReport
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"customRules":[{"AttributeName":"Carrier
Account","Company_Id":"97","Rule_Id":317,"CustomRule_Id":"686","MetricCatalog":"vw_StandardStats_Device","MeasurementCode":"Lookup","Denomination":"","Operato
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 14813
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:27:29 GMT


<input id="mainCat" name="mainCat" type="hidden" value="ADHOCREPORTS" />
<form action="/Notification/AddEditCustomRulePredicates" class="form-horizontal" data-ajax="true" data-ajax-method="POST
...[SNIP]...
```

```
<script>
var ruleInReports = '512,532,490,510,707,513,514,515,289,511,317'
var defaulrRules = '512,532,490,510,707,513,514,289'
var desc = 'sdfsdf'
var editedBy = 'Edited by ganesh.jagdale@aszroh.com on 05/03/2021 20:56:21 PM'
$(document).ready(function () {
//$(".customtooltip").popover({
// html: true,
// container: 'body',
// trigger: 'hover',

...[SNIP]...
```

6.3. https://portal.simetric.com/Notification/GetCustomRulePredicate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://portal.simetric.com**
Path:	**/Notification/GetCustomRulePredicate**

Issue detail

The following email address was disclosed in the response:

- rahil.shaikh@aszroh.com

Request

```
GET /Notification/GetCustomRulePredicate?customruleid=911&companynumber=simetric&ruletypeid=31 HTTP/2
Host: portal.simetric.com
Cookie: ARRAffinity=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df;
ARRAffinitySameSite=10bc9f9b89634ae526ead7649557fba3f1367c0c2f031640b8c28dbaae79e6df; ASP.NET_SessionId=23nizql1pu4oa4lq0g0mapjy; timezoneoffset=-330;
.AspNet.Cookies=eOHZDbGh08LvgowrWQLk2vrGfRWEkGC1yHiP-
w5L1tWv2eaHd6ugc0eIhfQq72LSjTBiHCXQbOwHBl3eXojjaqk6Br_L6Z1coSCAox9sQva0J2tzeeYI93TI82los55BsMLc27KkPfecL1gFHETFHUdjW9ud-
ZUfZeAhRFSzLgBFCvA8TFvMzfk_UuW32Q1GEDLFyAg_Yb3QCLDxvHOW0IaFSLHcgc1XlCJ4JjqP8TLEtiUODzXv_pFFq_PWZhCjAIpxwqtNBbmrGjynpor89CbV6SQyzTwK92EA6Tb76R
FBLLemuSMH1FcTB4_Otg-NBPfi_ndIrvC5juN2Ak7qAZ6Gja4zeRuBEPvM65og38JJ5wPsDwDx_yDqQyhOaNw2Gu5B9J2Vy4LM3z6nXPpyy-
tiPcZnFXqWVPgIpc7G1fPcmbp68SghjuOaPFEqWG3-mVxhIfOGo5udxcVAuQ6W18VEpflG58fSrxbPrk0ygvgjWTuplz4y6zrhOtBIw9iQ86hC9Z-ncUClWxGp3-
NUfQAdIa2Qyqx9O_XmjakjPQ_UyHqh3iDyQbgI_MRmJtS2yGoOec5h0OL43GwPTOZ152LHN480bQ8NcRwcnlButBxHz7S6gA6h2amEG5bv7a_jW_7YmRuBW8GgwnkCxbUUmxmB7b4jF
ViVUjGW4toOoPaFqGAoshq8AnxZ6H1_gVYeuk8ICb_v3a3uDJhn2q3kft81vk60sR-FX2SSK-Rojbme5wSZUKhGnRm2AzGd2zflxdg-Px0o0CKvaEsaAGiv2vzORqnZTpOuzRmUdO29w-
rN3Po4DW2_DdgUfy6y9KELt8e3SHHThFXgHf-iPKrvsQ
Sec-Ch-Ua: "Chromium";v="91", " Not;A Brand";v="99"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://portal.simetric.com/simetric/Notification/WatchLists
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/2 200 OK
Cache-Control: private, s-maxage=0
Content-Length: 7552
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Feature-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Date: Mon, 05 Jul 2021 07:32:51 GMT


<input id="mainCat" name="mainCat" type="hidden" value="WATCHLISTS" />
<form action="/Notification/AddEditCustomRulePredicates" class="form-horizontal" data-ajax="true" data-ajax-method="POST"
...[SNIP]...
<script>
var ruleInReports = ''
var defaulrRules = ''
var desc = ''
var editedBy = 'Edited by rahil.shaikh@aszroh.com on 05/13/2021 21:27:06 PM'
$(document).ready(function () {
//$(".customtooltip").popover({
// html: true,
// container: 'body',
// trigger: 'hover',

...[SNIP]...
```

Report generated by Burp Suite web vulnerability scanner v2021.6.2, at Mon Jul 05 13:27:55 IST 2021.